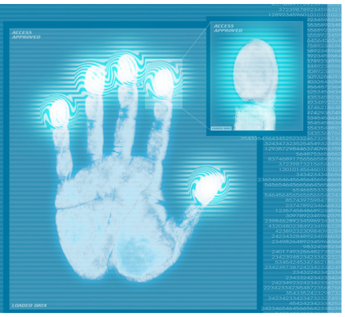


Chemical Sector Security Awareness Guide

A Guide for Owners, Operators, and Chemical Supply-Chain Professionals

September 2012

Homeland
Security

It is important to identify the response agencies with whom you will be working in your specific community and geographical region to build and enhance existing relationships before a security incident occurs. The list below is offered as a starting point.

Resource	Contact	Phone Number
Facility Security Officer		
Facility Safety Officer		
Facility Information Technology Manager		
City Law Enforcement		
County Law Enforcement		
State Law Enforcement		
Local Fire Service		
City Emergency Management		
County Emergency Management		
State Emergency Management		
Local Federal Bureau of Investigation (FBI) and Joint Terrorism Task Force	www.fbi.gov/contact/fo/fo.htm	
FBI Weapons of Mass Destruction (WMD) Coordinator at local FBI office		
U.S. Department of Homeland Security (DHS) Protective Security Adviser for this State/District	FOBAnalysts@HQ.dhs.gov	703-235-9349
Captain of the Port (if applicable)		
CFATS Regional Commander (if applicable)		
DHS Chemical Facility Anti-Terrorism Standards (CFATS) Tip Line		877-394-4347
CFATS Helpdesk (if applicable)	csat@dhs.gov	866-323-2957
DHS United States Computer Emergency Readiness Team (US-CERT)	www.us-cert.gov	888-282-0870
U.S. Coast Guard National Response Center (if applicable)	www.nrc.uscg.mil	800-424-8802
National Infrastructure Coordinating Center	NICC@dhs.gov	202-282-9201

Table of Contents

List of Tables

Purpose

The purpose of this document is to assist owners and operators in their efforts to improve security at their chemical facility. The goal is to make professionals working in the Chemical Sector aware of the security risk to the sector and to provide a list of activities or actions that they can take to reduce that risk. The information included in this document is not exhaustive but is an introduction only and is applicable for both regulated and non-regulated facilities. For more information on any of these topics, please send an e-mail to **ChemicalSector@dhs.gov**.

This guide would not be possible without the help of our partners. We would especially like to thank the Sector Coordinating Council, the Government Coordinating Council, and security professionals within the industry who take a proactive stance on security and who assisted us in preparing this document.

Distribution

The Chemical Sector Security Awareness Guide was prepared under the auspices of the U.S. Department of Homeland Security (DHS). For distribution information, contact **ChemicalSector@dhs.gov**.

Notice

This material does not constitute a regulatory requirement nor is it intended to conflict, replace, or supersede existing regulatory requirements or create any enforcement standard.

Introduction

After the September 11th attacks, the chemical industry immediately saw the need for increased security measures at chemical facilities and voluntarily began the process of reducing their security risk. While historically there have been no Federal regulations mandating security standards for the entire sector, Congress passed the Maritime Transportation and Security Act of 2002 (MTSA) to reduce the security risk on navigable waterways including certain chemical port facilities. More recently, in 2007, Congress passed legislation giving the U.S. Department of Homeland Security (DHS) authority to regulate chemical facilities that present "high levels of security risk."[1] The Chemical Facility Anti-Terrorism Standards (CFATS) established a risk-based approach to screening and securing chemical facilities, excluding those that MTSA and water/waste water treatment facilities cover. As the National Infrastructure Protection Plan (NIPP) outlines, security issues in the sector are also addressed through a public-private partnership between industry and all levels of government as well as interested stakeholders. DHS has invited members of the partnership to participate because each has a critical role to play in reducing security risk in the Sector.

Voluntary measures and new regulations mandating security measures at high-risk facilities are important in securing the sector. New threats to the continued reliability and integrity of all chemical infrastructure require everyone to be vigilant. In order to assist owners and operators in their efforts to increase security, this document contains baseline security information to raise facility-wide awareness of potential threats, detection methods, and reporting processes. This document also includes general information on the security threats that explosive devices and cyber vulnerabilities present. The underlying message of the guide stresses the importance of communication, not only within the facility, but also with local law enforcement agencies and emergency response personnel. A quick and coordinated response is an important factor in addressing and eliminating security threats.

[1] In April 2007, DHS published the Chemical Facility Anti-Terrorism Standards (CFATS) which require high-risk chemical facilities to complete security vulnerability assessments and implement site security plans that meet risk-based performance standards established by DHS. A facility that contains threshold quantities of a chemical of interest (COI), as identified in Appendix A to CFATS, must complete and submit to DHS a consequence assessment in order to determine if that facility is high risk. The COI were identified based on the belief that these chemicals, if released, stolen, diverted, or contaminated have the potential to inflict significant human life and health consequences. The Appendix A list of chemicals can be found at: **http://www.dhs.gov/xlibrary/assets/chemsec_appendixa-chemicalofinterestlist.pdf**

The Chemical Sector as a Potential Target

The chemical industry has been effective at leveraging their successful risk management approach to safety and applying the same process to address security. In addition, industry associations within the sector have developed guidance documents to improve security practices and raise security awareness. However, due to its size and business characteristics, the Chemical Sector[2] may be an attractive target[3] for attack for a number of reasons, including:

- Some chemical facilities contain large quantities of toxic, explosive, or flammable industrial chemicals. An attack on such a facility could cause fatalities, extensive injuries, severe physical destruction and panic, and generate heavy media attention. These are all key objectives of most terrorist groups.
- A variety of facilities in the Chemical Sector store, use, or process toxic, explosive, and flammable chemicals and chemical precursors. Terrorists may attempt to steal these chemicals in order to use them in a later attack at a different location. As regulated facilities implement measures to increase security, be aware that focus may shift to unregulated facilities that may be easier to access from a theft standpoint.
- Chemicals are bought and sold every day for a variety of purposes. It may be possible for terrorists to pose as legitimate customers in order to purchase or divert certain chemicals for use in an attack.
- As one of the largest exporting sectors in the United States, the chemical industry is a significant contributor to a strong and vibrant economy. Due to the wide variety of products the Chemical Sector produces and distributes, many other industries rely on the sector to sustain their business or provide service. Therefore, an attack on the Chemical Sector could have a very significant impact on the economy.

Although there is no credible, specific threat to the Chemical Sector at this time, it is important to remember that the threat picture is a snap shot in time. The threat is determined through intelligence and information from multiple sources at a given time, but is based on incidents that have already happened. It is therefore possible that the threat landscape will change rapidly and without warning. To that end, it is important that all security partners remain vigilant regarding chemical infrastructure security.

[2] The Chemical Sector is one of 18 critical infrastructure and key resource (CIKR) sectors of the U.S. economy that HSPD-7 established in 2003. The sector encompasses facilities that produce basic chemicals, specialty chemicals, agricultural chemicals, pharmaceuticals, and consumer end products.

[3] *The Chemical Sector: Potential Target for Attack, Theft, and Diversion of Materials*, U.S. Department of Homeland Security, Intelligence and Analysis Division and Federal Bureau of Investigation, Weapons of Mass Destruction Directorate, July 2009.

Identifying and Recognizing the Security Threat

While chemical facilities have been recognized as potential targets for terrorists,[4] in order for an attack to be successful, preparation is required. Whether an attacker follows a specific checklist or procedure, an attack will generally follow a cycle of events similar to those listed in the table to the right. Attackers need to be able to predict activity surrounding the facility through surveillance. When they target a site, they undertake surveillance to determine the strengths and weaknesses of the facility as well as to gather information concerning the number of personnel that typically respond to an incident. Therefore, some of the best returns on a facility's security investments can be realized by concentrating on protective measures and activities that can hinder attacker surveillance of the facility.

Attack Cycle

1. Target Selection
2. Surveillance
3. Final Selection
4. Planning/Surveillance
5. Attack Team Deployed
6. Zero Hour
7. Action/Attack

Surveillance can take place from a fixed or mobile site. Attackers typically carry out fixed surveillance from a concealed position but can also use disguises that would provide logical reasons for the attacker to be in the area, for example, a tourist, delivery man, or, in some cases, a demonstrator. An attacker may also conduct mobile surveillance to track the movements of an individual. Progressive techniques can complicate both types of surveillance. An attacker may observe the target from one position then withdraw for a time and resume surveillance from a different position. This will continue until the attacker determines the suitability of the target and identifies patterns and vulnerabilities in facility operations. A sophisticated surveillance operation may occur over a very long period of time from months to years and may be very difficult to detect.

However, there are several likely threat indicators that could be detected if a facility or operation was selected as a target. These indicators are associated with the following activities:

- Surveillance;
- Elicitation;
- Tests of security such as probing;
- Acquiring supplies;
- Suspicious people who don't belong;
- Dry runs or rehearsals; and
- Deployment.

Table 1 contains an expanded list of indicators for the first five activities.

[4] In this context, terrorist is synonymous with attackers or perpetrators, and refers to those who engage in premeditated threats or acts of violence (based on the definition of terrorism as defined in the 2009 National Infrastructure Protection Plan [NIPP], page 111).

Table 1. Indicators of a Possible Security Threat

Surveillance	Persons observed near the facility using or carrying video, camera, or observation equipment, especially using high-magnification lenses, or taking detailed notes of the facility.
	Persons with installation maps or facility photos/diagrams with specific areas highlighted or notes about the facility or personnel.
	Persons possessing or observed using night-vision devices near the perimeter of the facility or in the local area.
	Persons observed parking, standing, or loitering in the same area over several days for no apparent reason.
	Unusual recreational activities near the facility such as boating, hiking, or biking.
Elicitation	Reports of facility personnel being asked questions about the facility while off-site or after their normal workday.
	Reports of unsolicited phone calls to employees by individuals posing as researchers or officials requesting information about the company.
	Computer hackers attempting to access sites looking for personnel information, maps, or other types of facility-specific information.
Tests of Security	A noted pattern or series of false alarms requiring law-enforcement or emergency services response
	Sudden movement by people or vehicles when approached or observed by security personnel.
	Unfamiliar cleaning crews, utility workers, or other contract workers with passable credentials who attempt to access unauthorized areas.
	Unknown delivery personnel attempting to gain access to the facility, but claiming to be lost when challenged.
	Individuals representing themselves as government personnel (Federal, State, local) attempting to gain access to the facility or obtain sensitive information who cannot or will not present appropriate identification.
	Recent damage to a facility's perimeter fence, gate, perimeter lighting, closed-circuit televisions, or other security devices.
Acquiring Supplies	Theft of facility ID cards, uniforms, or vehicles with a facility logo.
Suspicious People/ Behavior	Seemingly legitimate groups showing up for facility tours at odd hours, on weekends, or holidays.
	Unknown individuals seen inside the facility or individuals not following basic facility protocols such as wearing an ID card or hard hat.
	Suspicious individuals going through the company's dumpster or trash looking for sensitive information.
	Unusual employee activity such as increased travel, unexplained disposable income, or decreased interactions with other employees.
	Employee trying to gain access to a restricted area such as a boiler room, mechanical room, or chemical storage room without going through proper procedures.
	Employee transporting boxes to and from the facility under unusual circumstances.

While surveillance provides the attackers with the best information on their potential target, it also offers the greatest opportunity for a facility to detect surveillance and take action to deter the attack. As Table 1 indicates, possible indicators of surveillance include such things as persons videotaping a facility, persons loitering in the area over several days, or unusual activities taking place near the facility. However, it is possible to make a facility less attractive to an attacker by introducing unpredictability into the security schedule. A potential attacker will note the unpredictable schedule during the surveillance stage. Too many variables in the attack plan decrease the likelihood of a successful attack and may cause an attacker to pick a different target.

Additionally, facility personnel can identify potential surveillance by:

- Identifying locations perpetrators must occupy to view security and/or vulnerabilities;
- Maintaining observation of these areas for suspicious activity; and
- Mitigating surveillance from these areas by repositioning closed-circuit television (CCTV) coverage, focusing security patrols in surveillance locations, or adjusting the environment to hinder surveillance.

Attackers may also try to elicit information about personnel, chemical shipments, or a facility's normal operating procedures. These inquiries would most likely occur in an informal setting outside of a facility employee's normal workday. This information would prove valuable to an attacker trying to test a facility's security.

The Chemical Sector is vigilant against theft and diversion, since certain chemicals are primary targets for illegal activities. However, other types of supplies or equipment would also be desirable for attackers to obtain, for example, official identification cards and badges or company uniforms. This type of equipment would make it easier to enter a secure or prohibited area. Therefore, organizations should be aware of individuals exhibiting peculiar behavior, asking unusual questions, or using odd language.

A "dry run" is often employed to work out the flaws in an attack plan. This can include everything from recording emergency response times to mapping entrance and escape routes or monitoring traffic lights and traffic flow. In the final stages, personnel may also notice people and supplies being positioned to commit the attack.

In addition to chemical manufacturing sites, the Chemical Sector also includes distribution facilities and transportation systems that move chemicals across the country. These facilities have unique characteristics that make them susceptible to a threat or attack. In addition, it may also be possible to detect suspicious activities while selling chemicals to potential customers.

Table 2 contains a list of suspicious activities that are pertinent to each of these segments in the chemical supply chain.

Table 2. Indicators of Suspicious Activities in the Chemical Supply Chain

Facilities Manufacturing Chemicals	Abnormal valves, connections, or piping that could be used to steal chemicals.
	Individuals or personnel with small containers not normally used at the facility such as barbecue tanks, cylinders, closed pails, or cans.
	Suspicious vehicles or persons monitoring hazardous materials shipments into and out of the facility.
Facilities Transporting or Distributing Chemicals	Abandoned trucks, cars, tank trucks, or unnecessary and unexplained delays in delivery or receipt.
	Truck, rail, or towboat personnel who do not have proper identification or who are acting suspiciously.
	Delivery or receipt of materials outside of normal operating hours and procedures.
	Inventory control problems including: • Irreconcilable discrepancies in quantity and quality of materials. • Missing or damaged container, truck, or tank car seals. • Discrepancies between seal numbers and shipping documents
	Unauthorized repackaging of chemical inventory from large containers, such as drums, to smaller containers. This may indicate illegal activity between company employees and truck driver/distributor.
	Contact with unknown individuals en route to shipment destination.
	Unauthorized or suspicious attempt to divert, delay, or reroute shipments.
Sales or Ordering of Chemicals	The party ordering the material cannot answer basic questions on material use, explanation for current use, normal end-use application, or safety and handling.
	The party ordering offers unusually favorable payment terms, such as a higher price, a higher lump-sum cash payment, or better interest rate than the prevailing market.
	An order of unusual material or quantities inconsistent with the customer's business or established ordering pattern.
	Requests for samples, particularly large samples (pails), of hazardous listed materials by new or unknown parties.
	Unexplained, unapproved, or new delivery location for sensitive materials to an existing customer or a reluctance to provide information on the location of end use.
	A transaction involving a third-party consignee that is unusual when compared to standard business practices.

Lastly, be aware that the chemical industry may be an attractive potential employer for employees, contractors, or service personnel with criminal intent. While many chemical companies have initiated criminal background checks for new employees, be aware that potential employees may use fake credentials or a fake identity in their application materials in order to gain employment at a chemical plant, a chemical distributor, or chemical transportation company. Also, ensure that contractors and service personnel have the proper facility pre-approval, and training or certification to perform the task they have been assigned before gaining access to sensitive production areas. Consider initiating escort procedures to ensure these temporary workers are escorted at all times, and restrict the tools, equipment, and cellular phones used in sensitive areas to only those required to perform the specific task.

General Awareness of Improvised Explosive Devices

The previous section discussed general indicators Chemical Sector employees should look for that may indicate a possible security threat. The threat itself, however, may take one of several forms including improvised explosive devices (IEDs), vehicle-borne improvised explosive devices (VBIEDs), or cyber attacks.

The threat of explosive attacks is of concern considering terrorists' proven ability to make, obtain, and use explosives, the ready availability of IED components, and the relative technological ease with which attackers can fashion an IED. Attacks using IEDs have become increasingly sophisticated in recent years, and are a preferred tactic for a number of reasons:

- IEDs can be relatively inexpensive to create;
- Great skill is not always required to produce an IED; and
- IEDs can be built into a high-yield weapon. When successfully detonated, these devices produce dramatic results and draw much public attention.

A variety of different packaging may contain or conceal IEDs, for example, pipes, tubes, suitcases, handbags, postal mail, backpacks, trash cans, or computers. The package is important since it is used to deliver the IED without raising suspicion. In addition, the container can contribute to the damage caused by the explosion by fragmenting when the explosion occurs. Below are some examples of packaging used in IEDs.

Examples of Packaging

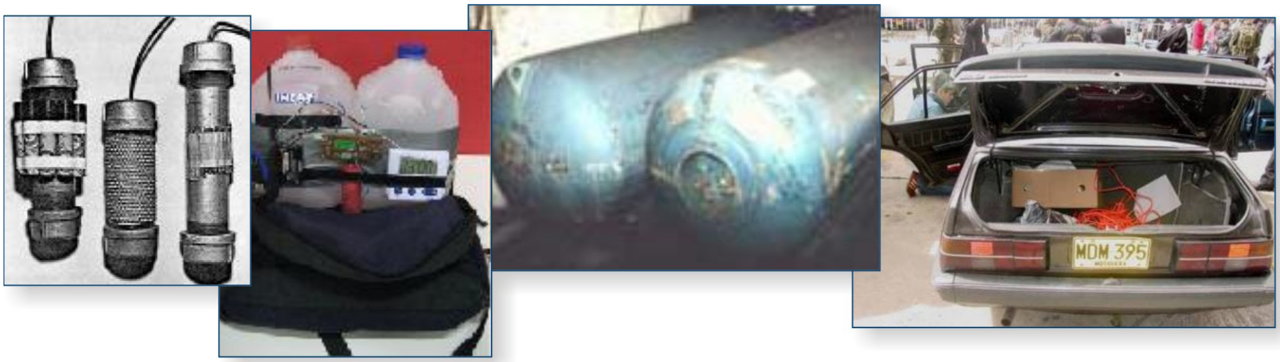


Table 3. Common Oxidizers, Acids, and Fuels Used in IEDs[5]

Common oxidizers, acids, and fuels are used to create IEDs. Oxidizers serve as a source of oxygen to support a combustion-like reaction; fuels consist of anything that can readily react with oxygen in a manner which produces heat. The more complex explosives require the addition of an acid for synthesis.

Common Oxidizers	
$NaClO_3$	Sodium Chlorate
$KClO_3$	Potassium Chlorate
$KClO_4$	Potassium Perchlorate
NH_4ClO_4	Ammonium Perchlorate
H_2O_2	Hydrogen Peroxide
BaO_2	Barium Peroxide
NH_4NO_3	Ammonium Nitrate
KNO_3	Potassium Nitrate
$KMnO_4$	Potassium Permanganate
$K_2Cr_2O_7$	Potassium Dichromate
$Ca(OCl)_2$	Calcium Hypochlorite
HNO_3	Nitric Acid
$Pb(IO_3)_2$	Lead Iodate

Acids	
H_2SO_4	Sulfuric Acid
HCl	Hydrochloric Acid
HNO_3	Nitric Acid
$C_6H_8O_7$	Citric Acid

Common Fuels	
Nitrobenzene	Sawdust
Nitromethane	Methanol
Nitrocellulose	Ethanol
	Urea
Gas	Glycerine
Diesel	Ethylene Glycol
Kerosene	
Naphtha	Aluminum (**Al**)
Carbon Black	Magnesium (**Mg**)
Charcoal	Zirconium (**Zr**)
Sugar	Copper (**Cu**)
Wax/Paraffin	Magnalium (**Mg/Al - 50/50**)
Acetone	Phosphorus (**P**)
Methyl Ethyl Ketone	Sulfur (**S**)
Hexamine	Antimony Trisulfide (**Sb_2S_3**)
Shellac	
Rosin	

[5] This table is adapted from data available from *Improvised Explosive Threat Card: Investigators Bulletin 2006-4.1*, U.S. Department of Justice, Federal Bureau of Investigation, Bomb Data Center.

Some of the chemicals listed in Table 3 may be regulated under CFATS. DHS developed the CFATS Appendix A Chemicals of Interest list to include chemicals that present one or more security issue. The Appendix A list is available for review at: **http://www.dhs.gov/xlibrary/assets/chemsec_appendixa-chemicalofinterestlist.pdf**

While IEDs are typically hidden in containers, employees at chemical facilities that keep work areas neat and clean will be more likely to notice items that are out of place or don't belong. This includes observing when common chemical containers, such as five gallon pails or drums, are not in their usual places.

If employees find a suspicious package or item that may be an IED, they should:

- Not move or interfere with it in any way;
- Not use radios/cell phones in the immediate vicinity of the suspicious item;
- Move away to a safe distance;
- Prevent others from approaching; and
- Notify the proper authorities.

Attackers can use a variety of chemicals, fertilizers, and petroleum products to produce explosive devices. Table 3 contains a number of chemicals categorized by common oxidizers, acids, or fuels that attackers may use in combination to produce an IED. Oxidizers serve as a source of oxygen to support a combustion-like reaction; fuels consist of anything that can readily react with oxygen in a manner which produces heat. The more complex explosives require the addition of an acid for synthesis. While this is not an exhaustive list, many of these items are available at chemical facilities and may be susceptible to theft.

Again, one of the best defenses against the theft and misuse of such chemicals is general security awareness. Employees that handle chemicals typically receive training on their proper use and storage. Therefore, be suspicious of anyone who is not handling or using chemicals correctly, as well as unusual activity around chemical storage areas. Also be suspicious of customers ordering chemicals that are unable or are unwilling to explain the use of the chemicals they are ordering.

An increasingly popular form of IED is the Vehicle-Borne Improvised Explosive Device (VBIED). Vehicles are attractive because

- Larger explosive loads can be transported to almost any target location;
- Vehicle features, such as tinted windows, make it easy to hide explosives; and
- Larger vehicles are still allowed in parking garages, a favorite target of terrorists.

Table 4 includes a list of potential indicators for suspicious vehicles.

Of the various forms of IEDs, attackers prefer VBIEDs because they are an effective way to deliver large quantities of explosives without drawing immediate suspicion, while also producing large numbers of fatalities and casualties. In addition, with the vehicle acting as the container, fragmentation of the vehicle can cause a substantial portion of the associated damage. The explosion from any IED produces a shock wave or blast wave in the surrounding medium which can be lethal within a certain range. Persons within this lethal range would be susceptible to significant injury. An additional concern of an IED for those facilities located in an urban setting is the increased likelihood that existing structures may channel the blast out into the surrounding community.

Table 4. Potential Indicators of a Suspicious Vehicle

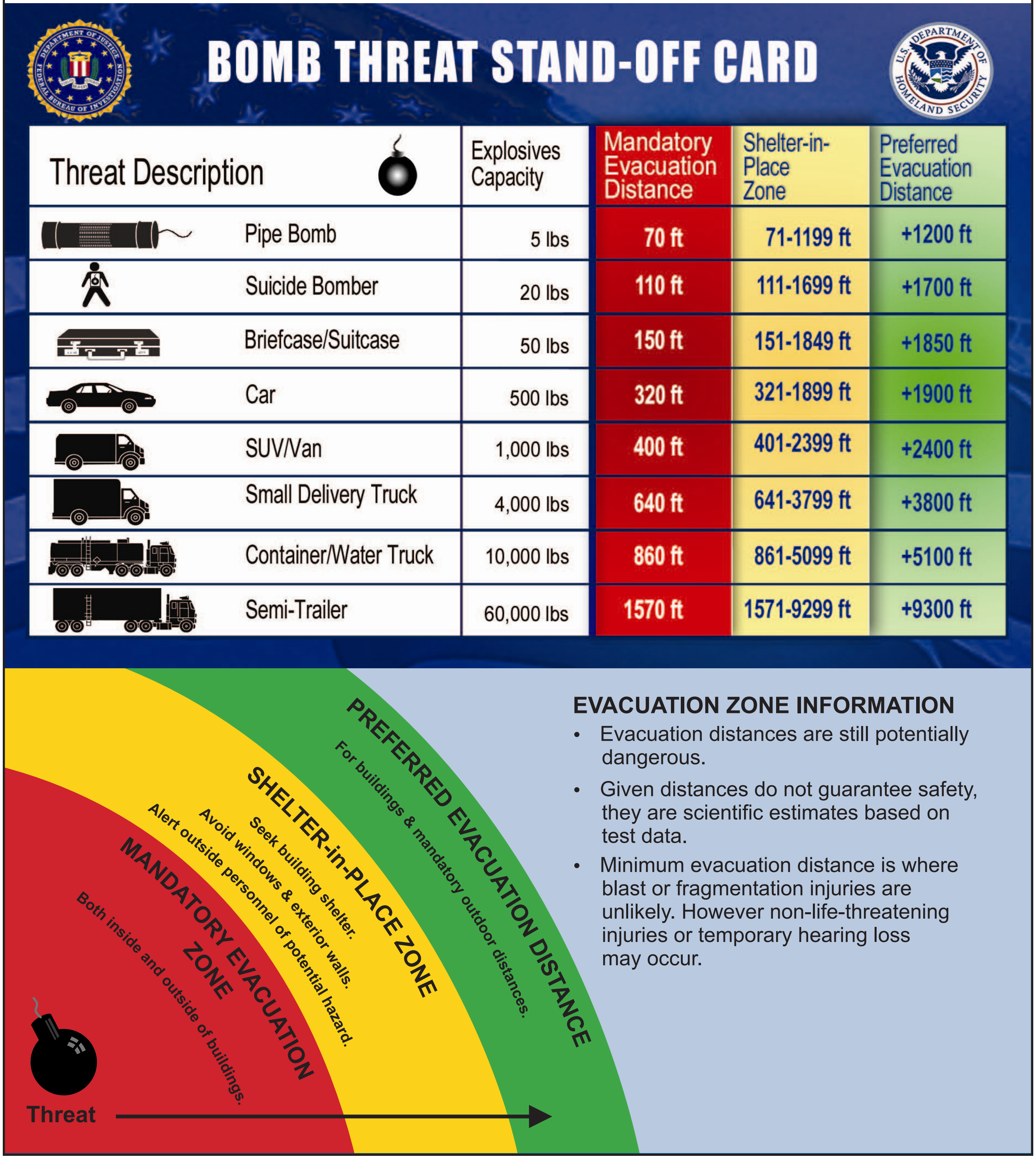
Heavy sagging vehicle (rear-weighted).
Illegally parked or parked near authorized vehicle entrances or crowded access points.
Covered or tinted windows.
Large containers on seats or cargo area: bags, boxes, barrels, or tanks.
License plates removed or altered.
Odor of gasoline, propane, acids, or chemicals.
Visible wires, switches, batteries, or antennae inside or on vehicle.
Cargo concealed with tarp or blanket.
Holes in the vehicle body to hide explosives and then crudely covered.
Evidence that an interior door panel has been removed to hide explosives.
Presence of powder or other granular material left when explosive material was loaded into the vehicle.
Recent painting of the vehicle to cover body alterations.
Vehicles or suspicious containers parked or located near fences and roads that are also near chemical storage tanks or rail cars.

Table 5 contains a variety of IED types and corresponding safe evacuation distances should the device explode. Note that increasing the explosive capacity of a VBIED by a factor of 8 (500 lbs to 4000 lbs) would require only a doubling of the safe evacuation distance. However, no matter what kind of IED is involved, one of the best protective measures against an explosion is distance. The further an individual is from the point of detonation, the less forceful the blast wave will be, and the less chance of being killed or injured by debris from the explosion.

Additionally, employees should always be aware of the normal pattern of vehicle traffic at their facility. Facilities typically interact with the same transportation companies and truck drivers on a routine basis. Rental trucks are typically not used by chemical companies and employees should view them as suspicious within facility boundaries. Also, transport regulations for hazardous chemicals require vehicles to be kept clean and free of chemical residues. Employees should consider the presence of such residue on transportation vehicles as suspicious.

Table 5. Safe Evacuation Distances for Selected Improvised Explosive Devices (IEDs)

This table illustrates the explosive capacity of several different types of IEDs and the corresponding minimum evacuation distances considered to be safe. Note that increasing the TNT equivalent explosive capacity of a VBIED by a factor of 8 (500 lbs to 4,000 lbs) would require only a doubling of the evacuation distance.



BOMB THREAT STAND-OFF CARD

Threat Description	Explosives Capacity	Mandatory Evacuation Distance	Shelter-in-Place Zone	Preferred Evacuation Distance
Pipe Bomb	5 lbs	70 ft	71-1199 ft	+1200 ft
Suicide Bomber	20 lbs	110 ft	111-1699 ft	+1700 ft
Briefcase/Suitcase	50 lbs	150 ft	151-1849 ft	+1850 ft
Car	500 lbs	320 ft	321-1899 ft	+1900 ft
SUV/Van	1,000 lbs	400 ft	401-2399 ft	+2400 ft
Small Delivery Truck	4,000 lbs	640 ft	641-3799 ft	+3800 ft
Container/Water Truck	10,000 lbs	860 ft	861-5099 ft	+5100 ft
Semi-Trailer	60,000 lbs	1570 ft	1571-9299 ft	+9300 ft

MANDATORY EVACUATION ZONE

Both inside and outside of buildings.

SHELTER-in-PLACE ZONE

Seek building shelter.

Avoid windows & exterior walls.

Alert outside personnel of potential hazard.

PREFERRED EVACUATION DISTANCE

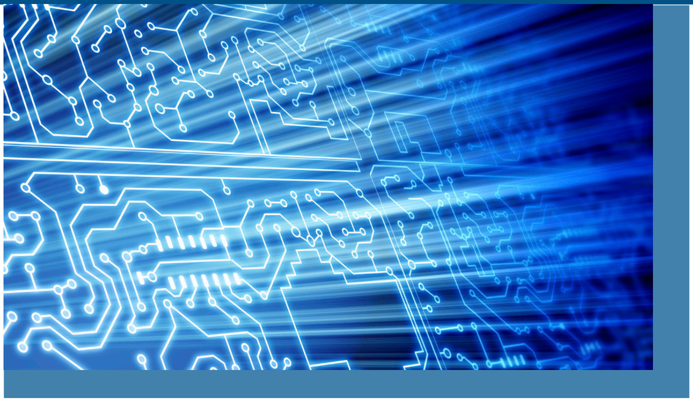
For buildings & mandatory outdoor distances.

Threat

EVACUATION ZONE INFORMATION

- Evacuation distances are still potentially dangerous.
- Given distances do not guarantee safety, they are scientific estimates based on test data.
- Minimum evacuation distance is where blast or fragmentation injuries are unlikely. However non-life-threatening injuries or temporary hearing loss may occur.

Cybersecurity



The chemical industry is highly dependent on information technology (IT) for its communications and operations. Technological advances that promote better efficiency and more automation within the industry also make information security an increasingly important issue. Information security is more than just the desktop PC you use every day. It also includes the network access that allows vendors and engineers to troubleshoot and update systems remotely.[6] This is one reason the cyber infrastructure is increasingly susceptible to attack without the correct policies in place.

Personnel surety is an important aspect of securing cyber systems at chemical facilities. Many companies in the sector mitigate the risk of coercion or insider threat by using policies, practices, and technologies that protect the linkage of critical plant systems with corporate networks. Sector stakeholders use secure authentication technology to restrict access based on roles and clearances while employing proper policies to delete user accounts once an employee's relationship with a chemical company is terminated. Table 6 lists a number of actions employees can observe to increase cybersecurity at chemical facilities. The table also includes a list of measures that company management or IT specialists may already have implemented in order to protect information networks from a cyber attack.

[6] Information Security in *Security Guidelines for the Petroleum Industry*, American Petroleum Institute, April 2005.

Table 6. Cybersecurity - What You Can Do

Employees
Create complex passwords by using a combination of numbers, symbols, and letters (uppercase and lowercase).
Change your passwords regularly, every 45 to 90 days.
Do NOT give any of your user names, passwords, or other computer/Web site access codes to anyone.
Do NOT open e-mails or attachments from unknown individuals or e-mails with unusual subject lines.
Make electronic and physical back-ups or copies of all your most important work.
Do NOT install or connect any personal software or hardware to your organization’s network or hardware without permission from your IT department.
Do NOT download or store sensitive information on an external storage device without proper authorization.
Do NOT leave company laptop computers unattended while on business travel. This includes leaving them in cars, hotel rooms, etc. For travelers going through airport security, consider placing a label or other recognizable feature on the exterior of the laptop computer so that it can be easily recognized by company employees and retrieved quickly.
Report all suspicious or unusual problems with your computer to your IT department.
Management and IT Department
Establish clear policies and procedures for employee use of your organization’s information technologies.
Establish clear policies and procedures for protecting e-commerce cyber systems from online customers, including initiating a “know your customer” program.
Implement technical defenses: firewalls, intrusion-detection systems, and Internet content filtering.
Update your antivirus software regularly. The period between updates depends upon the availability of updates from manufacturers, the risk to systems, and the operating environment.
Regularly download vendor security patches for all of your software.
Change the manufacturer’s default passwords on all of your software.
Monitor, log, and analyze successful and attempted intrusions on systems and networks.

Attackers have used a variety of methods to infiltrate cyber systems and are continually developing new ones as technology advances. It is therefore very important to report any incidents that appear suspicious while using your company's computing system. Table 7 lists examples of such suspicious incidents.

Table 7. Suspicious Cyber Incidents

System Failure/ Disruption	Employees, customers, suppliers, or partners are unable to access the company/facility system or Web site.
Suspicious Questioning	Individuals attempt to gain information in person, by phone, mail, or e-mail, regarding the configuration or cybersecurity posture of the company/facility Web site, network, software, or hardware.
Suspicious E-mails	Individuals at your company/facility receive suspicious e-mails that include unsolicited attachments or requests for sensitive personal or organizational information.
Unauthorized Access	Individuals attempt to gain unauthorized access to company/ facility data, including contractors who attempt to gain unauthorized access to automated industrial control systems.
Unauthorized Changes/ Additions	Unauthorized changes or additions made to company/facility system hardware, firmware, or software characteristics without IT department's knowledge, instruction, or consent.
Unauthorized Use	Unauthorized individuals use the company/facility system to process or store data. Unauthorized individuals would include former employees, customers, suppliers, or other former partners.

For more information on the latest cybersecurity issues or for additional resources, visit the U.S. Computer Emergency Readiness Team Web site at: **www.us-cert.gov**.

Reporting Incidents

Once suspicious activities have been detected, it is important to contact the proper authorities in a timely manner and to relay accurate information.

In the event of an emergency, call 911 and report to local police. When reporting suspicious activity, personnel should follow company procedures and also contact the local Federal Bureau of Investigation Joint Terrorism Task Force (JTTF) about the suspicious activity (contact information available at: www.fbi.gov/contact/fo/fo.htm).

In addition, consider the following actions:

If your facility is regulated by the Maritime Transportation and Security Act (MTSA), contact the National Response Center at:

- Phone: 800-424-8802

To report suspicious cyber activity, incidents, and vulnerabilities affecting critical infrastructure control systems, contact the U.S. Computer Emergency Readiness Team (US-CERT) at:

- General cyber activity: **soc@us-cert.gov**
- Control system related cyber activity: **ics.cert@dhs.gov**
- Phone: 888-282-0870

Otherwise, facilities should report suspicious activity to the National Infrastructure Coordinating Center (NICC) at:

- E-mail: **nicc@dhs.gov**
- Phone: 202-282-9201

Timeliness is critical because the likelihood of apprehending the suspicious person(s) is greatest when the report is made immediately upon identifying the suspicious activity. In addition, as time passes, it allows the suspicious person(s) to alter their appearance to render them unrecognizable to the one witnessing the suspicious activity.

Accurate information is also critical. Embellishing or exaggerating the facts may hamper an investigation. When reporting a suspicious activity, explain why the activity seemed suspicious even if the rationale is that the activity was “out of the ordinary.” However, a detailed explanation of why the activity seemed out of the ordinary is very important.

When reporting suspicious behavior, it is important to include as much information as possible. It is helpful to keep the following questions in mind when reporting an incident:

Who?	Describe the person or persons involved in the suspicious activity. Include as much of the following information as possible: **Persons** • Gender • Size or build • Height • Race or ethnicity • Peculiar features such as scars, marks, tattoos, missing limbs • Hair color, hair style, and length, including facial hair • Eye color • Clothing style and description from head to toe **Vehicle** • Color, make, model, and year • Type of vehicle: passenger car, SUV, or van • License plate number and state • Damage or unusual markings such as designs or company names • Accessories such as running lights, unusual wheels/tires, or trailer
What?	Describe the suspicious activity. Is there an immediate threat? What was stolen or missing? • What is the likelihood of harm to personnel or infrastructure? • Can stolen item(s) be used alone or in combination with other materials to form a destructive device? • Are there recommended precautions to be taken when dealing with the stolen item(s)? • Are there specialists or experts that would be appropriate to contact?
When?	Be as accurate as possible when reporting the time the suspicious activity occurred. • Is it still in progress? • If not, how long ago did the activity occur?
Where?	Give your location, the location of the suspicious activity, and the location of the suspects.
Why?	Explain why the activity being reported seems suspicious. What might be the target of the activity?
How?	Describe how the activity was carried out. How did you discover the activity? How did you discover items were missing?

If reporting a suspicious package…

What?	…does it look like? …is the size? …is the shape? …is the color? …is the type of packaging material? …does it smell like? …is marked on it? …is attached to it or protruding from it?

It is extremely important for a facility and the response community to develop a personal relationship so that they can conduct joint training and exercises, establish ongoing mutual education, and establish an information-sharing process. This level of preparedness is a fundamental element in countering or deterring an attack. Surveillance of a facility will likely reveal the strength of the relationship with a responding agency or department, and could prove to be a valuable deterrent to attack. In addition, when these relationships are established, it is possible for the facility to report the kind of information that local law enforcement needs, and in turn, local law enforcement can share information the facility would find useful in situations where no immediate action is required.

Another important element of preparedness is knowing where to go for information regarding security concerns. Table 8 lists a number of resources available to the private sector providing the latest information and updates on security incidents.

If additional information regarding a specific security issue of concern is not available on the sites listed in Table 8, e-mail the NICC requesting more information at **nicc@dhs.gov**.

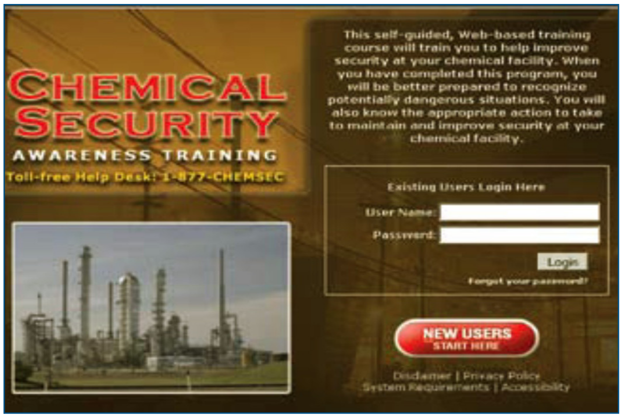
Table 8. Resources for Security Information and Updates

Source	Description
Homeland Security Information Network – Critical Sectors (HSIN-CS)	HSIN-CS is the primary information-sharing platform for the Chemical Sector. It provides alerts and incident bulletins when events occur. HSIN-CS enables DHS, critical Sector security partners, and chemical supply chain professionals to communicate, coordinate, and share information in support of the Sector Partnership Framework. Primary objectives of HSIN-CS are to generate effective risk management decisions and to encourage collaboration and coordination on plans, strategies, protective measures, and response and recovery efforts among government and owners and operators. E-mail **ChemicalSector@dhs.gov** for registration information.
DHS Daily Open Source Infrastructure Report ***http://www.dhs.gov/dhs-daily-open-source-infrastructure-report***	The DHS Daily Open Source Infrastructure Report (Daily Report) is collected each week day as a summary of open-source published information concerning significant critical infrastructure issues. Each Daily Report is organized by the critical infrastructure sectors and key assets the National Infrastructure Protection Plan defines. Subscribe via the website to get e-mail updates when new reports are posted.
InfraGard ***http://www.infragard.net***	InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the Federal Bureau of Investigation and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the U.S. InfraGard Chapters are geographically linked with FBI Field Office territories.
HOMEPORT ***http://homeport.uscg.mil***	HOMEPORT is the official U.S. Coast Guard information technology system for maritime security created to provide information and services to the maritime community and the public over the Internet. Coast Guard Federal Maritime Security Coordinators use Homeport as a primary means for the day-to-day management and communication of non-sensitive and sensitive port security matters with Area Maritime Security Committee members, commercial vessel and facility owners and operators, government partners, as well as the public.
United States Computer Emergency Readiness Team (US-CERT) ***http://www.uscert.gov***	Congressional and Presidential authorities assign US-CERT the responsibility to serve as the focal point for analysis and warning related to the Nation's cyber infrastructure. US-CERT collaborates with public and private sector partners to collect information on cyber activity through submissions of incident reports, suspicious files/malware, cyber intelligence, and monitoring data feeds.

Chemical Sector-Specific Agency Voluntary Security Programs

The goal of this guide is to make professionals working in the Chemical Sector aware of the security risk to the sector and to provide a list of activities or actions that they can take to reduce that risk. DHS, as the Chemical Sector-Specific Agency (SSA), has been assigned responsibility for overseeing voluntary security efforts. The Chemical SSA has collaborated with private sector partners to develop a wide range of voluntary programs in an effort to lower the security risk in the sector and to provide easy-to-use accessible tools. Following is a list of programs that specifically target the security risks discussed in this guide as well as other programs designed to share security-related information.

- The **Homeland Security Information Network – Critical Sectors (HSIN-CS)** is the primary information-sharing platform for the Chemical Sector. It provides alerts and incident bulletins when events occur. HSIN-CS enables DHS, critical sector security partners, and chemical supply chain professionals to communicate, coordinate, and share information. Primary objectives of HSIN-CS are to generate effective risk management decisions and to encourage collaboration and coordination on plans, strategies, protective measures, and response and recovery efforts among government and owners and operators.


CHEMICAL SECURITY
AWARENESS TRAINING
Toll-free Help Desk: 1-877-CHEMSEC
Login
Forgot your password?
NEW USERS START HERE
Disclaimer | Privacy Policy
System Requirements | Accessibility

This self-guided, Web-based training course will train you to help improve security at your chemical facility. When you have completed this program, you will be better prepared to recognize potentially dangerous situations. You will also know the appropriate action to take to maintain and improve security at your chemical facility.

Existing Users Login Here

User Name:

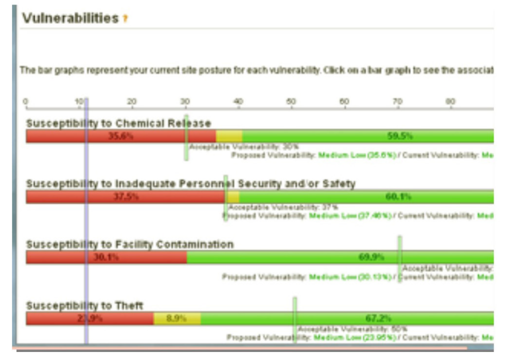
Password:

- The **Web-Based Chemical Security Awareness Training Program** is an interactive free tool based on industry best practices and designed to increase security awareness in chemical facilities nationwide, whether they are involved with the manufacture, transportation, or storage of chemicals. The program also includes a module for employees of chemical facilities falling under the MTSA. Upon completion, a certificate is awarded to the participant. To access the training, go to: **https://chemicalsecuritytraining.dhs.gov.**

- **Tabletop Exercises** are unclassified and adaptable exercises creating an opportunity for public and private critical infrastructure stakeholders and their public safety partners to address gaps, threats, issues, and concerns with incident response and recovery. The various exercises contain a number of incident-specific resources as well as the suite of documents needed to conduct a Homeland Security Exercise and Evaluation Program compliant TTX. TTXs available on DVD include: Bomb Threat; Workplace Violence/Active Shooter; and Major Earthquake

- The **Security Seminar and Workshop Series** encourages facility owners and operators and their security partners to collaborate in an interactive seminar and discussion forum. The outcomes of this collaboration include progress in information sharing about all-hazards threats, vulnerabilities, and consequences, as well as enhanced communication between facilities and their local emergency response teams. Current scenario is an Improvised Explosive Device (IED), and it is coordinated and facilitated with the Office of Bombing Prevention (OBP).

- The **Unclassified Security Briefing and Suspicious Activity Reporting Teleconference** is co-hosted by the Chemical SSA and Oil and Natural Gas subsector for facility owners and operators, plant managers, and supply chain professionals. The teleconference, occurring the fourth Thursday of every month, provides the opportunity for the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) and US-CERT to brief the sectors on significant changes to the threat environment, results of recent terrorism investigations, and other reported suspicious incidents.



Vulnerabilities

The bar graphs represent your current site posture for each vulnerability. Click on a bar graph to see the associat

0
10
20
30
40
50
60
70
80
Susceptibility to Chemical Release
35.6%
59.5%
Acceptable Vulnerability: 30%
Proposed Vulnerability: Medium Low (35.6%) / Current Vulnerability: Me
Susceptibility to Inadequate Personnel Security and/or Safety
37.5%
60.1%
Acceptable Vulnerability: 37%
Proposed Vulnerability: Medium Low (37.46%) / Current Vulnerability: Med
Susceptibility to Facility Contamination
30.1%
69.9%
Acceptable Vulnerability:
Proposed Vulnerability: Medium Low (30.13%) / Current Vulnerability: Med
Susceptibility to Theft
23.9%
8.9%
67.2%
Acceptable Vulnerability: 50%
Proposed Vulnerability: Medium Low (23.95%) / Current Vulnerability: Me

- The **Voluntary Chemical Assessment Tool** (VCAT) is a secure, Web-based application and self-assessment tool. Once users enter their data, the tool allows owners and operators to identify the facilities' current risk level using an all-hazards approach, and facilitates a cost-benefit analysis by allowing them to select the best combination of physical security counter measures and mitigation strategies to reduce overall risk.

- The **Chemical Sector Industrial Control Systems Security Resource DVD** was compiled by the chemical industry in partnership with DHS, and is designed to assist owners and operators in addressing Industrial Control Systems (ICS) security. The DVD contains a wealth of training and reference information, including: DHS Cybersecurity Evaluation Tool (CSET); cybersecurity tabletop exercise; suggested cybersecurity procurement language for controls systems; ICS security training resource guide; ICS standards and guidelines; and information on cyber threats and mitigation strategies.

For a more complete list of programs and resources, visit our Web site at **www.dhs.gov/chem-voluntary-resources.** For questions or for additional information, please contact **ChemicalSector@dhs.gov**.

Appendix A: DHS Cybersecurity Programs

DHS' National Cyber Security Division (NCSD) serves as the national focal point for cybersecurity and collaborates with numerous components within DHS to provide all sector partners with cybersecurity resources, cross-sector information-sharing support, and the technical assistance necessary to best prepare for and respond to cyber events. Following is a list of additional programs and activities that may be of interest to cyber specialists in the Chemical Sector:

NCSD Control Systems Security Program (CSSP) was established to reduce control system risks within and across all critical infrastructure sectors by coordinating efforts among Federal, State, local, and tribal governments, as well as control systems owners, operators, and vendors.

Industrial Control Systems Joint Working Group (ICSJWG) is part of the CSSP's effort to bring together stakeholders involved in the protection of critical infrastructure assets as it relates to control systems and cybersecurity. This working group will facilitate the collaboration of stakeholders to accelerate the design, development, and deployment of more secure industrial control systems.

The United States Computer Emergency Readiness Team (US-CERT) is a partnership between DHS and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the Nation.

US-CERT is charged with protecting our nation's Internet infrastructure by coordinating defense against and response to cyber attacks. US-CERT responsibilities include the following:

- Analyzing and reducing cyber threats and vulnerabilities;
- Disseminating cyber threat warning information; and
- Coordinating incident response activities.

US-CERT interacts with Federal agencies, industry, the research community, State and local governments, and others to disseminate reasoned and actionable cybersecurity information to the public.

Visit the US-CERT Web site at www.us-cert.gov.

Appendix B: Supplemental Information

Information on the Security Threat

The Chemical Sector: Potential Target for Attack, Theft, and Diversion of Materials, U.S. Department of Homeland Security, Intelligence and Analysis Division and Federal Bureau of Investigation, Weapons of Mass Destruction Directorate, July 2009.

Agricultural, Chemical, and Petroleum Industry Terrorism Handbook, Department of Justice, Federal Bureau of Investigation, http://www.mcpr-cca.org/downloads/FBIAgChemHandbook.pdf

Chemical and Biological Outreach Program, pamphlet, revised 2006, Department of Justice, Federal Bureau of Investigation.

Homeland Security Student Reference: Surveillance Detection Training for Commercial Infrastructure Operators and Security Staff, Armor Group International Training, Inc., April 2007.

Improvised Explosive Threat Card: Investigators Bulletin 2006-4.1, Department of Justice, Federal Bureau of Investigation, Bomb Data Center.

Seven Signs of Terrorist Activity, http://www.mcpr-cca.org/downloads/FBIAgChemHandbook.pdf.

Terrorist Surveillance Indicators, http://www.scnus.org/page.html?ArticleID=105214.

Vehicle Born Improvised Explosive Device – VBIED: The Terrorist Weapon of Choice, Henry Morgenstern, http://www.nationalhomelandsecurityknowledgebase.com/Research/International_Articles/VBIED_Terrorist_Weapon_of_Choice.html.

Homeland Security Information Bulletin, *Potential Indicators of Threats Involving Vehicle- Borne Improvised Explosive Devices (VBIEDs)*, U.S. Department of Homeland Security, May 15, 2003, http://www.sifma.org/uploadedfiles/services/bcp/homeland%20security%20information%20bulletin%20051303.pdf.

Guidance Documents:

Roadmap to Secure Control Systems in the Chemical Sector and additional resources and tools are available at: www.chemicalcybersecurity.com.

Protect Your Workplace: Guidance on Physical and Cybersecurity and Reporting of Suspicious Behavior, Activity, and Cyber Incidents, U.S. Computer Emergency Readiness Team, brochure available at www.US-CERT.gov.

Information Security in *Security Guidelines for the Petroleum Industry*, American Petroleum Institute, 2005 and available at: http://new.api.org/policy/otherissues/upload/Security.pdf.

Background on the Chemical Industry

2009 Guide to the Business of Chemistry, American Chemistry Council, 2009.

Chemical, Biological, and Radiological Events, and the Critical Infrastructure Workforce: Final Report and Recommendations by the Council, January 2008, http://www.dhs.gov/xlibrary/assets/niac/niac_CBR_FINAL_REPORT.pdf

Chemical Sector Regulations and Partnerships

Critical Infrastructure: Chemical Security, http://www.dhs.gov/critical-infrastructure-chemical-security. (This is the DHS Web site designed to inform the private sector about the Chemical Facility Ant-Terrorism Standards (CFATS).)

Critical Infrastructure: Sector Partnership, http://www.dhs.gov/critical-infrastructure-sector-partnerships.

National Infrastructure Protection Plan, http://www.dhs.gov/national-infrastructure-protection-plan.

Reducing Chemical Terrorism Risk: The Role of Public-Private Partnerships, Thomas Lehrman, Remarks at the Fourth Annual Toxic Industrial Chemicals/Toxic Industrial Materials Symposium, July 12, 2006, http://merln.ndu.edu/archivepdf/wmd/State/69690.pdf

Appendix C: Chemical Sector Coordinating Council

Member Associations

Agricultural Retailers Association

American Chemistry Council

American Coatings Association

American Fuel & Petrochemical Manufacturers

Chemical Producers and Distributors Association

Compressed Gas Association

Crop Life America

International Liquid Terminals Association

Institute of Makers of Explosives

International Institute of Ammonia Refrigeration

National Association of Chemical Distributors

Society of Chemical Manufacturers and Affiliates

The Chlorine Institute

The Fertilizer Institute

Appendix D: Chemical Sector Government Coordinating Council

Member Departments and Agencies

Department of Homeland Security

Chemical Safety Board

Department of Commerce

Department of Defense

Department of Energy

Department of Justice

Department of Labor

Department of State

Department of Transportation

Environmental Protection Agency

Office of the Director of National Intelligence

State, Local, Tribal, and Territorial Government Coordinating Council

Appendix E: List of Acronyms and Abbreviations

ATF — Bureau of Alcohol, Tobacco, Firearms and Explosives

CCTV — Closed-circuit television

CFATS — Chemical Facility Anti-Terrorism Standards

CIC — Chemical Industry Council

CIKR — Critical Infrastructure Key Resources

COI — Chemical of interest

CSSP — Control Systems Security Program

DHS — U.S. Department of Homeland Security

FBI — Federal Bureau of Investigation

GCC — Government Coordinating Council

HITRAC — Homeland Infrastructure Threat and Risk Analysis Center

HSIN-CS — Homeland Security Information Network – Critical Sectors

ICSJWG — Industrial Control Systems Joint Working Group

IED — Improvised explosive device

IT — Information Technology

JTTF — Joint Terrorism Task Force

MTSA — Maritime Transportation Security Act of 2002

NCSD — National Cyber Security Division

NICC — National Infrastructure Coordinating Center

NIPP — National Infrastructure Protection Plan

PSA — Protective Security Advisor

SCC — Sector Coordinating Council

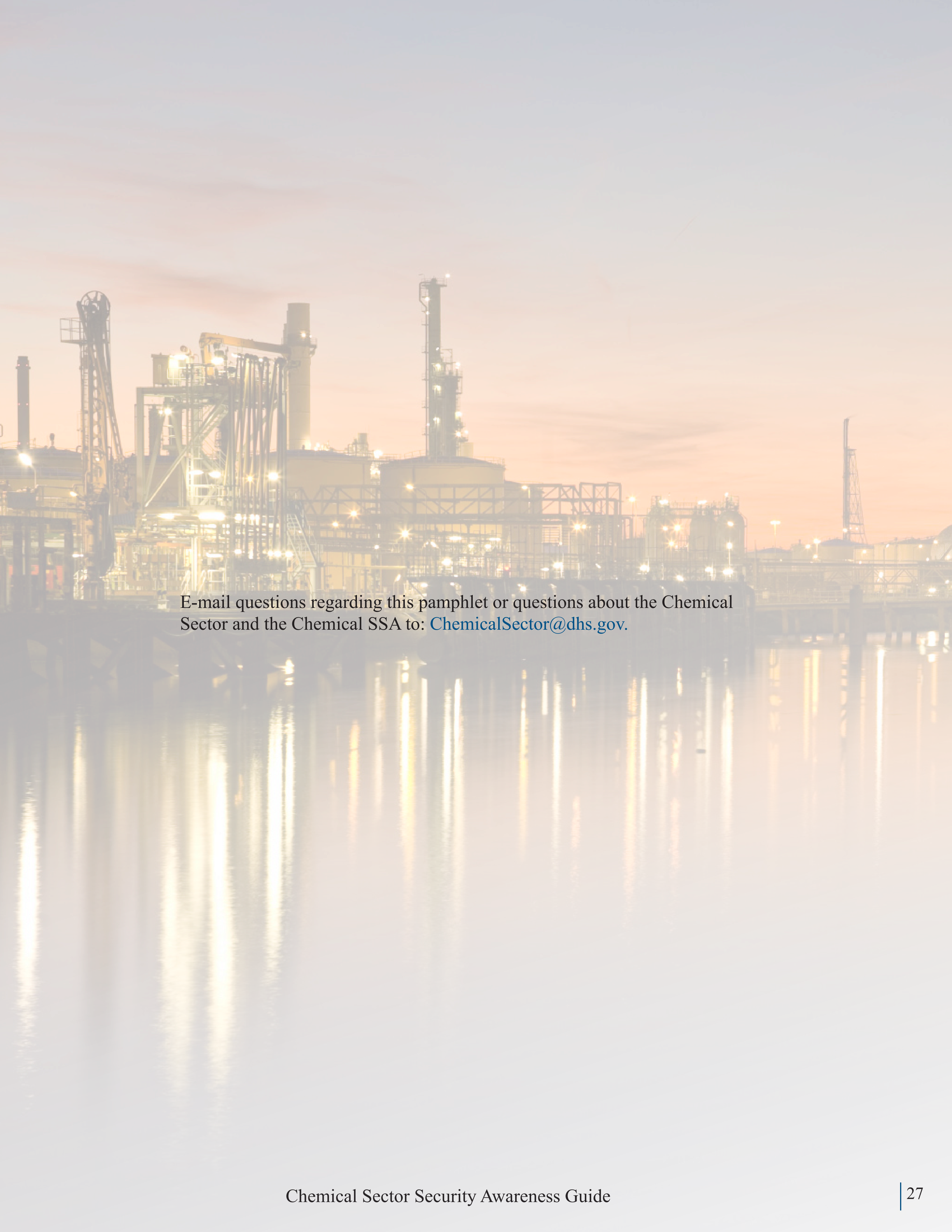
SSA — Sector-Specific Agency

US-CERT — United States Computer Emergency Readiness Team

VBIED — Vehicle-borne improvised explosive device

VCAT — Voluntary Chemical Assessment Tool

WMD — Weapon of mass destruction



E-mail questions regarding this pamphlet or questions about the Chemical Sector and the Chemical SSA to: ChemicalSector@dhs.gov.